

**67-5-22. Identity theft reporting information system -- Internet website and database -- Access -- Maintenance and rulemaking -- Criminal provisions.**

(1) There is created within the Office of the Attorney General the Identity Theft Reporting Information System (IRIS) Program to establish a database and Internet website to:

- (a) allow persons in the state to submit reports of identity theft;
- (b) assist the Office of the Attorney General in notifying state and local law enforcement agencies of reports of identity theft;
- (c) provide assistance and resources to victims of identity theft;
- (d) provide a centralized location where information related to incidents of identity theft may be securely stored and accessed for the benefit of victims of identity theft; and
- (e) provide public education and information relating to identity theft.

(2) (a) The Internet website shall be maintained by the Office of the Attorney General and shall be made available to the public and to victims of identity-related crimes.

(b) The Internet website shall:

(i) allow a victim of an identity-related crime to report the crime on the website and have the victim's report routed to the appropriate law enforcement agency for the jurisdiction in which the crime occurred; and

(ii) provide public education and information relating to identity theft.

(c) The Internet website may be expanded to provide other identity-related services to victims according to the procedures of Subsection (4).

(3) (a) The Department of Technology Services shall administer and maintain the database established under this section in an electronic file or other format as established by the department.

(b) (i) The database shall be maintained for the purpose of identifying victims of identity theft who have filed a report with the program established under this section, and may contain the personally identifiable information for each victim, which may include the following information related to an incident of identity theft:

- (A) the victim's name, address, email addresses, and telephone numbers;
- (B) the victim's Social Security number and other identifying information;
- (C) the victim's financial institution information, account numbers, and transaction information;
- (D) the victim's benefit information;
- (E) the victim's credit account information;
- (F) the victim's loan information;
- (G) the victim's employment information;
- (H) the victim's Internal Revenue Service or tax information;
- (I) the victim's utility service information;
- (J) information concerning legal matters or collections related to the incident;
- (K) information concerning unauthorized or illegal transactions, denied credit, stolen identification, and all other unauthorized actions related to the identity theft; and
- (L) any other information related to the incident of identity theft that the victim or the Office of the Attorney General elects to include in the database.

(ii) The database shall record and maintain:

(A) identification information for each person who requests or receives information from the database;

(B) a record of the information that is requested or received by each person who requests or receives information from the database; and

(C) a record of the date and time that any information is requested or provided from the database.

(c) Information in the database is considered to be the property of the Office of the Attorney General, and retains any classification given it under Title 63G, Chapter 2, Government Records Access and Management Act.

(4) The Department of Technology Services, with the approval of the Office of the Attorney General, may make rules to:

(a) permit the following persons to have access to the database:

(i) federal, state, and local law enforcement authorities, provided that the authority is acting within a specified duty of the authority's employment in enforcing laws;

(ii) participating merchants and financial institutions, provided that the merchant or institution has entered into an access agreement with the Office of the Attorney General; and

(iii) other persons, to be established by rule, provided that the person's access to the information is necessary and reasonable to accomplish the purposes of the program as provided in Subsection (1);

(b) define and enforce limitations on access to information via the Internet website or in the database; and

(c) establish standards and procedures to ensure accurate identification of individuals that are requesting or receiving information from the Internet website or the database.

(5) (a) In addition to the penalties provided under Title 63G, Chapter 2, Government Records Access and Management Act, a person may not knowingly and intentionally release or disclose information from the database in violation of the limitations provided under Subsection (4)(a).

(b) A violation of Subsection (5)(a) is a third degree felony.

(6) (a) A person may not obtain or attempt to obtain information from the database by misrepresentation or fraud.

(b) A violation of Subsection (6)(a) is a third degree felony.

(7) (a) A person may not knowingly and intentionally use, release, publish, or otherwise make available to any other person or entity any information obtained from the database for any purpose other than those specified under Subsection (4)(a).

(b) Each separate violation of Subsection (7)(a) is a third degree felony.

Amended by Chapter 161, 2008 General Session